FLOCK INFORMATION SHARING AGREEMENT

FLOCK Equipped Law Enforcement Agencies

FOR SHARING LAW ENFORCEMENT INFORMATION

Santa Maria Police / California Highway Patrol

I. OVERVIEW

a. Introduction:

The purpose of this "Agreement" is to outline conditions under which the Agency Parties will share and use "scanned plate" and "hot list" information. Each Agency Party shall be required to maintain their own FLOCK services.

b. Background:

FLOCK is a computer-based system that utilizes emerging technology to capture a color image, as well as an infrared image, of the license plate of a vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file," also known as a "hot list", and can contain information on stolen or wanted vehicles as well as vehicles associated with Amber Alerts, warrant subjects, and agency defined-information.

FLOCK cameras can be mobile (on a trailer) or on fixed positions such as freeway overpasses or traffic signals. FLOCK Safety systems have all the necessary equipment to scan plates, notify the user of a vehicle hit, and upload the scanned plate information into the FLOCK repository for retention and research.

Agencies entering into this agreement hereinafter referred to as "Agency Parties," realizing the mutual benefits to be gained by sharing information, seek to share scanned plate and hot list information. The specific technological means for securely connecting these informational sources will be approved by agency FLOCK Safety administrators.

Each Agency Party separately contracts with Flock Group, Inc. This Agreement shall also be governed by those separate agreements with Flock Group, Inc.

Each Agency Party shall adhere to applicable laws, regulations, and their own policies related to the usage of ALPR information.

II. AUTHORIZED RELEASE OF INFORMATION

a. Sharing of Information:

Each Agency Party authorizes the release of scanned plate and hot list information residing in their respective databases or networks to other Agency Parties as permitted by law. An Agency Party that does not want certain

information made available to any other Agency Party is responsible for ensuring that the information is not available for data exchange.

b. Limitation on Information Sharing:

Scanned plate and hot list information shall only be shared with or released to other Agency Parties. Only authorized employees who have an approved login and password ("Authorized Users"), and a need and/or right to know, will be allowed to access any other Agency Party's scanned plate and hot list information.

c. Liability:

Each Agency Party is solely responsible for any and all claims (including, without limitation, claims for bodily injury, death, or damage to property), demands, obligations, damages, actions, causes of action, suits, losses, judgments, fines, penalties, liabilities, costs and expenses (including, without limitation, attorney fees, disbursements and court costs), and "claims" of every kind and nature whatsoever, arising in any manner by reason of the negligent acts, errors, omissions, or willful misconduct incident to the performance of this Agreement, including the use or alleged or actual misuse of scanned plate and hot list information by that Party, its officers, agents or employees, this is to include data breaches.

d. Indemnification:

To the fullest extent permitted by law, each Agency Party receiving shared information shall indemnify, defend and hold harmless Source Agency, and its directors, officers, and employees from and against all liabilities (including without limitation all claims, losses, damages, penalties, fines, and judgments, associated investigation and administrative expenses, and defense costs, including but not limited to reasonable attorneys' fees, court costs and costs of alternative dispute resolution) regardless of nature or type that arise out of, pertain to, or relate to a breach of this agreement or the negligent, reckless, or willful misconduct of the Agency Party receiving information or the acts or omissions of an employee, agent or subcontractor of said Agency Party.

III. INFORMATION OWNERSHIP

a. Ownership:

Each Agency Party retains control of all information in its FLOCK repository. Each Agency Party is responsible for creating, maintaining, updating, and deleting records in its own repository according to its own retention policies. Each Agency Party shall use reasonable efforts to ensure the completeness and accuracy of its data.

b. Release of Information:

Agency Parties to this agreement hereby represent and warrant they are entitled to receive shared information contemplated by this Agreement. Agency Parties and authorized users shall release or make available information accessed from the FLOCK repository only to persons or entities authorized to receive FLOCK information.

c. Unauthorized Requests:

If an Agency Party receives a request for information in the FLOCK repository by anyone who is not authorized to receive information from the FLOCK repository, that Agency Party shall refer the request to the law enforcement agency that originated the requested information ("Source Agency").

d. Public Record Requests, Subpoenas, and Court Orders:

Any Agency Party receiving a public records request, subpoena, or court order ("Legal Request") for information in the FLOCK repository not authored by or originated by that Agency Party shall immediately provide a copy of the Legal Request to the Source Agency, prior to providing a response to the Legal Request.

IV. UNDERSTANDING ON ACCURACY OF INFORMATION

a. Accuracy of Information:

Agency Parties agree that scanned plate and hot list information consists of information assumed to be accurate. Agency Parties will participate in routine testing sessions to validate and ensure that its information is accurate. However, data inaccuracies can arise for multiple reasons (e.g., entry errors, misinterpretation, outdated data, etc.). It shall be the responsibility of the Agency Party requesting or using the data to confirm the accuracy of the information with the Source Agency prior to taking any enforcement-related action.

b. Timeliness of Hotlist Data:

Each Agency Party shall determine the frequency with which its hot list data will be refreshed. Since changes or additions to hot list data do not get updated on a real-time basis Agency Parties recognize that information may not always be timely and relevant. It shall be the responsibility of the requesting Agency Party to confirm the timeliness and relevance of the information with the Source Agency. Additionally, a data refresh schedule will be made available by each system administrator to enable a user to determine the potential timeliness of each Agency Party's data. Agency Parties shall not store shared hot list data on any system for more than a 24-hour period without refreshing it.

V. USER ACCESS

a. Login Application Process:

Each Agency Party's system administrator is responsible for management of user accounts at that Agency Party. Each Agency Party agrees that all authorized users shall be limited to current employees who are legally authorized to review criminal history data for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency system administrator. The Agency system administrator shall have discretion to deny or revoke individual access.

b. Login Assignment:

Each Authorized User will be issued a user login and a default password by the Agency system administrator. Authorized Users may be assigned to groups that have different levels of access rights based on the level of restriction of the information.

c. Termination of Logins:

Each Agency system administrator is responsible for timely removal of any login accounts as Authorized Users leave the Agency, no longer qualify for access into the system, or are denied access by the Agency system administrator for any other reason.

d. Intended Use:

Each Authorized User agrees that scanned plate, hot list information, and the networking resources are to be used solely for law enforcement purposes only and consistent with the law. Authorized Users shall not use or share the information for any unethical, illegal, criminal, or commercial purpose. Pursuant to California Government Code Section 3, Chapter 17.25 (commencing with section 7284) federal, state or local law enforcement agencies shall not use any non-criminal history information contained within the database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. sections 1373 and 1644.

e. Limitations on Use of Logins:

An Authorized User shall not access information in a FLOCK Safety Repository by using a name or password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

f. Audit Trail:

Each transaction on the FLOCK Safety repository is to be logged, and an audit trail created. Each Agency system administrator shall conduct an internal audit on a periodic basis to ensure information is reasonably up to date and user queries are made for legitimate law enforcement purposes only.This information shall be recorded and retained to allow the system administrator to complete the internal audit. Each system administrator shall maintain the audit trail pursuant to the retention policies of that Agency Party. Requests for transaction logs shall be made in writing to the Agency system administrator, who shall provide the logs to the requesting party within a reasonable amount of time.

VI. CONFIDENTIALITY OF INFORMATION

a. Information Confidentiality:

Information in the FLOCK Safety repository is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information in the FLOCK Safety repository. Otherwise, the information shall be kept confidential.

b. Internal Requests for Information:

An Authorized User who receives a request from a non-authorized requester for information in the FLOCK Safety repository shall not release that information, but may refer the requester to the Source Agency.

c. Removal or Editing of Records:

Agency Parties shall determine their own schedule for record deletion and other edits to their own data. This will be determined by policy, legal requirements, storage, and technic l capability.

VII. SYSTEM ACCESS

a. Network Access:

Access to scanned plate and hot list information will be provided via such method that is mutually acceptable to the Agency Parties.

b. System Availability:

The FLOCK Safety repository shall operate 24 hours a day, seven days a week, with downtime limited to those hours required for any necessary maintenance activities.

VIII. AGREEMENT TERMS

a. Term:

This Agreement will commence on the date that it is executed by all Agency Parties. It will terminate only as allowed by Section IX.

b. Amendments:

Any change in the terms of this Agreement shall be incorporated into this Agreement by a written amendment properly executed and signed by the person authorized to bind the Agency Parties.

c. Controlling Law and Venue:

Any dispute that arises under or relates to this Agreement (whether contract, tort, or both) shall be adjudicated according to the laws of the State of California.

d. Severability:

If any term or portion of this Agreement is held to be invalid, illegal, or otherwise unenforceable by a court of competent jurisdiction, the remaining provisions of this Agreement shall continue in full force and effect.

IX. TERMINATION

Either Agency Party to this Agreement may terminate this Agreement upon giving the other Agency Party at least ten (10) days written notice prior to the effective date of such termination, which date shall be specified in such notice.

X. SIGN-OFF ON EXECUTION OF AGREEMENT

By executing this agreement, each Party acknowledges that it has received a copy of this agreement, and will comply with its terms and conditions. The person executing this Agreement certifies that the person is authorized by its Party to execute this Agreement and legally bind its Party to the terms herein. This Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

IN WITNESS WHEREOF, this agreement is executed by the parties on the last signed below:

CITY OF SANTA MARIA

Chief of Police

Date: 7-30-24

California Highway Patrol

Date: 7/29/24

APPROVED AS TO FORM:

(Asst.) City Attorney

Risk Manager